IMPLEMENTATION GUIDANCE

Enforcement of DOE Classified Information Security Requirements Under Title 10, Code of Federal Regulations, Part 824

March 2006

United States Department of Energy
Office of Special Operations
Office of Security Operations
Office of Security and Safety Performance Assurance

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

A SYNOPSIS: EVALUATION AND PROCESSING OF CIVIL PENALTIES FOR CONTRACTOR VIOLATIONS OF CLASSIFIED INFORMATION SECURITY

Title 10, Code of Federal Regulations, Part 824 (10 CFR Part 824) was published by the Department of Energy (DOE) to implement Section 234B of the Atomic Energy Act of 1954, 42 U.S.C. 2282b. Section 234B stipulates that a contractor or subcontractor to the DOE who violates any rule, regulation, or order relating to the safeguarding or security of Restricted Data, other classified information, or sensitive information shall be subject to a civil penalty (fine) not to exceed $100,000 per offense. In publishing 10 CFR Part 824, DOE has determined that civil penalties under Part 824 will only be assessed for violations of requirements for the protection of classified information (Restricted Data, Formerly Restricted Data and National Security Information). The rule does not include civil penalties relating to failure to protect sensitive but unclassified information.

SCOPE

The regulation applies to entities that have entered into contracts with DOE, rather than the individual employees of contractors and subcontractors. Contractors and their subcontractors are held responsible for the acts of their employees who fail to observe rules, regulations or orders. *Civil penalties will not be assessed against individual employees.*

The Office of Security and Safety Performance Assurance (SSA) has primary responsibility for enforcing this regulation as it applies to DOE contractors and subcontractors.

ENFORCEABLE RULES, REGULATIONS AND ORDERS

Currently, violations of requirements to protect classified information found in the following rules and directives could result in 10 CFR Part 824 action:

- 10 CFR Part 1016, *Safeguarding of Restricted Data* (this rule only applies to Access Permit holders)
- 10 CFR Part 1045, *Nuclear Classification and Declassification*
- DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management*
- DOE Manual 470.4-2, *Physical Protection*
- DOE Manual 470.4-3, *Protective Force*
- DOE Manual 470.4-4, *Information Security*
- DOE Manual 470.4-5, *Personnel Security*
- DOE Manual 470.4-6, *Nuclear Material Control and Accountability.*

In addition, failure to comply with a compliance order issued by the Secretary of Energy dealing with the protection of classified information could be subject to a 10 CFR Part 824 action.

PROCESS

The process outlined in 10 CFR Part 824 is designed to be a comprehensive and fair administrative process that will allow for discussions with the contractor prior to a formal notice of violation that may contain a proposed fine. If the Department proposes to fine a contractor, the contractor is always given the opportunity to respond and to request a hearing.

A number of factors are considered in determining the appropriate enforcement action. Violations of classified protection requirements are assigned a severity level that is determined based on an evaluation of the specific facts and circumstances of each case. Other factors to be considered include the frequency and willfulness of the violation(s) and whether the contractor has taken appropriate and effective corrective measures to resolve the problem. The rule also provides for reduction of any proposed civil penalty when the contractor has self-reported the violation.

The steps in the process are described below.

Identification

Violations of classified information security requirements are identified and reported, via the established incident reporting and management program. Additionally, classified information security incident identification may occur during the conduct of other security activities (e.g., security self-assessments, periodic surveys, independent oversight inspections, and Office of the Inspector General and Government Accountability Office activities).

Investigation

SSA develops further information by means of document reviews, interviews, and other activities, including signing, issuing and serving subpoenas. The SSA Office of Special Operations (SP-23) will conduct any additional investigation that is needed to develop the facts surrounding the violation. On the basis of this information, the SSA will make the decision whether to proceed with further actions. This decision takes the same factors into consideration as the assignment of the severity level: the degree of the contractor's responsibility; the training and experience of those involved; past performance of the contractor; and the duration of the violation. A group of violations with the same severity level and similar underlying circumstances may be aggregated for further actions.

Incident Review Meeting

Upon completion of the investigation/inquiry regarding an incident of noncompliance with a requirement for protection of classified information the matter, a meeting will be held to review the issue(s). The meeting will be held to review the facts and make a determination as to whether or not to proceed with an enforcement action under 10 CFR Part 824. The meeting will be convened by the Director, SSA and composed of representatives from SSA, the Headquarters Program Office and the DOE Field Element having responsibility for the contractor believed to be in non-compliance, and either the Office of General Counsel or the NNSA Office of General Counsel.

Enforcement Conference

After the completion of inquiry or investigation activities and the conclusion that a violation occurred and warrants initiation of the 10 CFR Part 824 enforcement process, the Director, SSA convenes an informal Enforcement Conference. This conference is held with Departmental representatives and representatives of the contractor involved to: ensure the accuracy of facts; discuss the violation and its cause and significance; and present corrective actions and the schedule required for remedial activities. Mitigating or aggravating circumstances and other pertinent information are obtained that will help determine the proper enforcement action.

If the Director, SSA determines that the issue's significance is low and the issue does not warrant a notice of violation, or that the non-compliance has been corrected, the Director may issue a notice closing out the matter without an Enforcement Letter, or may issue an Enforcement Letter that addresses the noncompliance and explains the required corrective actions. Upon successful completion of the terms of an Enforcement Letter, the matter will be closed by the Director.

Preliminary Notice of Violation

If the Director determines that a violation warranting 10 CFR Part 824 processing has occurred, the proceedings for imposing a civil penalty begin with a written Preliminary Notice of Violation (PNOV) which is sent by certified mail, return receipt requested in accordance with 10 CFR Part 824. For NNSA cases the PNOV will be issued by the Administrator, NNSA. This notice contains:

- The date, facts, nature, and date of each act or omission constituting the alleged violation.
- The particular provision(s) violated.
- The proposed remedy for each alleged violation, including the amount of any proposed civil penalty.
- A statement of the right to reply to the PNOV.

Reply

After receiving the PNOV, the contractor has the opportunity to respond in writing within 30 days. If the contractor fails to respond, the PNOV will become a Final Notice of Violation (FNOV). The contractor may respond in several ways:

- Admit the violation, waive its right to contest the notice of preliminary violation, and pay the amount assessed.

- Admit the violation but contest the proposed penalty.

- Admit the violation and assert mitigating circumstances that would change the amount of the proposed penalty.

- Deny that the violation occurred and provide justification that the preliminary notice of violation is incorrect.

If the contractor concedes that the violation occurred (i.e., selects one of the first three options listed above), it must describe corrective steps to be taken and the expected results, remedial actions being implemented to prevent recurrence, and the date that full compliance will be achieved.

The written reply must contain a statement of all relevant facts regarding the alleged violation, including:

- Any facts that support the denial.
- Extenuating or mitigating circumstances.
- Authorities (rules, regulations, etc.) that support the position.
- Answers to any questions contained in the preliminary notice.
- Copies of all relevant documents.

DOE then evaluates the contractor's response and makes one of several determinations:

- No violation occurred.

- The violation occurred and the civil penalty should be mitigated either partially or in full.

- The violation occurred and the civil penalty is appropriate (even if mitigating circumstances were asserted).

If the evaluation determines that the violation occurred, a Final Notice of Violation (FNOV) is issued.

Final Notice of Violation

If, after consideration of the response submitted by the contractor, the Director finds that the violation occurred or continues to occur, a FNOV is issued within 30 calendar days from the time the reply is received. For cases involving the NNSA, the FNOV is issued by the Administrator, NNSA. This notice contains:

- The determined violation.
- The amount of civil penalty imposed.
- Further actions necessary or available.
- Notice of a right to request a hearing under 10 CFR Part 824.8.

The notice is deemed final 15 days after it is issued if it does not contain a civil penalty. If it does contain a civil penalty, the contractor must submit one of the following within 30 days of issuance:

- A waiver of further proceedings: The final notice is deemed a final enforceable order. Unless additional time is granted, the penalty set forth must be paid within 60 days of filing the waiver.

- A request for a hearing under 10 CFR Part 824.8: The hearing process is described below.

- A notice of intent to proceed under 234A.c.(3) of the Atomic Energy Act: The civil penalty is assessed, and the procedures of the Act are followed.

Hearing

The procedures for a hearing are specified in 10 CFR Part 824.8, which describes the selection and duties of the hearing counsel and the hearing officer. This section also describes the rights of the contractor to be represented by counsel to be present during the hearing: to testify, present evidence through witnesses or documents, and cross-examine witnesses; and to rebut evidence and physical records. A transcript of the hearing is made, and appropriate procedures are used to prevent unauthorized disclosure of classified information.

In the hearing, DOE has the burden of proving by a preponderance of evidence that the violation occurred and the proposed civil penalty is appropriate. The contractor has the burden of defending itself against the allegations set forth in the final notice. The hearing officer determines each matter of controversy upon a preponderance of the evidence.

Decision

If the hearing officer determines that a violation has occurred and a civil penalty is appropriate, the initial decision establishes the amount of the civil penalty based on several factors: nature, circumstances, extent, and gravity of the violation(s); violator's

ability to pay; effect of the penalty on the contractor's ability to do business; history of prior violations; and degree of culpability. The initial decision includes a notice that it constitutes a final order 30 days after the filing of the decision unless the Secretary files a notice of review.

If the Secretary of Energy files a notice of review, additional proceedings may be conducted, the matter may be remanded, or the civil penalty assessed in the initial decision may be modified. The contractor against which the civil penalty is assessed by the final order shall pay the full amount within 60 days unless the Director agrees otherwise. If payment is not made as required, DOE will institute an action in the appropriate district court to recover the amount of the penalty.

Assessment of Penalty

The civil penalty is a means through which DOE emphasizes the need for compliance with classified information security requirements, emphasizes the necessity of lasting remedial action, and deters future violations. The civil penalty also emphasizes the DOE requirement that contactors identify, report, and take corrective action when violations occur. A civil penalty will be proposed for Severity Level I and II violations, and may be imposed for Severity Level III violations when previous corrective actions have failed.

Adjustment Factors

DOE assesses civil penalties to emphasize the importance of compliance with classified information security requirements and to deter future violations. The goal is to ensure that contractors identify, report, and correct deficiencies in their programs before DOE discovers them. DOE therefore takes into consideration the circumstances of each case – considering the promptness, comprehensiveness, appropriateness, timeliness, and initiative displayed by the contractor's corrective action – when offering incentives in the form of adjustment factors.

These adjustment factors may result in a reduced civil penalty for violations promptly identified, reported, and effectively corrected by the contractor. However, if corrective actions are ineffective, or if violations are repeated, flagrant, or indicate a serious breakdown in management controls, the statutory maximum of penalty of $100,000 per violation per day may be assessed.

DOE normally reduces the amount of the civil penalty when contractors self-identify noncompliance. In evaluating this option, the following factors are considered: time elapsed and number of prior opportunities to identify the violation; effectiveness of contractor control in preventing or identifying the deficiency; whether the discovery was a result of self-monitoring; extent of DOE involvement in the discovery; and promptness and completeness of reporting.

However, DOE does not generally allow a reduction in penalties for this self-identification when an event occurs that discloses violations of which the contractor

should have been cognizant. The key is whether the contractor should have detected and addressed the noncompliance that contributed to the event.

CHAPTER 1: GENERAL

1.1 Purpose

This document provides detailed operational procedures used to implement the Department of Energy (DOE) *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations* as published in Title 10, Code of Federal Regulations, Part 824 (10 CFR Part 824). A copy of this rule is included for ready reference in Appendix A to this document. If necessary, supplemental procedures will be issued for the implementation of the civil penalties for failure to protect Unclassified Controlled Nuclear Information (UCNI) as described in Title 10, Code of Federal Regulations,1017.

1.2 Uses

This document contains both requirements and guidance. Procedural requirements are applicable to the Security Enforcement Staff and support personnel. Guidance describes the normal or expected course of action, but permits flexibility to deviate as needed for the particular circumstance.

The Department will exercise discretion in determining the disposition of any potential enforcement action, which may vary from the guidance in this procedure. It should be recognized that these procedures are internal to the Security Enforcement Staff and by extension the Federal and Contractor Security Incident Coordinators. This document is written in a flexible manner to maximize accommodation of each case and circumstance; therefore, if the Security Enforcement Staff and Security Incident Coordinators do not specifically follow the guidance and requirements as outlined in this document, their actions do not provide the basis to invalidate any enforcement action.

In general, all records and correspondence related to a pending enforcement action prior to the issuance of a Preliminary Notice of Violation (PNOV) are considered Official Use Only (OUO), Exemption 5, and are not subject to disclosure under the Freedom of Information Act (FOIA).

CHAPTER 2: ROLES, RESPONSIBILITIES AND AUTHORITIES

2.1 Director, Office of Security and Safety Performance Assurance (SSA)

The Director, SSA, has been assigned the responsibility by the Deputy Secretary of Energy to implement the Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations (10 CFR Part 824) in the case of non-NNSA contractors; in the case of NNSA contractors the Director, SSA makes a recommendation to the NNSA Administrator (see below). Throughout this document, the term Director, refers to the Director, SSA.

The Director ensures that the Secretary of Energy or designee will be notified, in advance, of the potential issuance of all Enforcement Letters or PNOVs. In addition, consultation with the Secretary is required before enforcement action is taken in any of the following cases:

- Any proposed enforcement action to impose civil penalties in an amount equal to or greater than $100,000
- Any proposed enforcement action that involves a Severity Level I violation
- Any enforcement action that the Director, SSA, concludes warrants the Secretary's involvement
- Any proposed enforcement action on which the Secretary asks to be consulted.

2.2 NNSA Administrator

The Administrator shall act after consideration of the Director, SSA's recommendation. If the Administrator disagrees with the Director's recommendation and the disagreement cannot be resolved by the two officials, the Director, SSA may refer the matter to the Deputy Secretary for resolution.

The Administrator has the responsibility to sign issue, serve, or take the following actions that direct NNSA contractors or subcontractors: subpoenas, orders to compel attendance, disclosures of information or documents obtained during an investigation or inspection, PNOVs and Final Notices of Violation (FNOVs.

2.3 Security Enforcement Staff

The Director, SSA, has designated the Office of Special Operations within the Office of Security Operations as the action office for security enforcement activities. This includes the following tasks:

- Evaluating compliance failures including, but not limited to incidents of security concern reported pursuant to DOE M 470.4-1, *Safeguards and Security Program Planning and*

Management, information reported to the Incident Tracking Analysis Capability (ITAC), survey, inspection, and special safeguards and security reports.

- Analyzing incident reports (or other noncompliance source documents).

- Recommending to the Director and the Administrator NNSA, as appropriate, whether to conduct an investigation and/or initiate enforcement actions.

- As directed, investigating potential violations of classified information security requirements as identified by internal or external sources, and conducting and preparing investigative reports with appropriate recommendations up to and including the recommendation of enforcement actions. If there is reason to believe a potential for criminal violation has occurred, DOE may refer the matter to the Attorney General of the United States for investigation.

- Coordinating and participating in Enforcement Conferences.

- Preparing all recommended enforcement action documents (e.g., Compliance Orders, Enforcement Letters, PNOVs and FNOVs) and appropriate transmittal letters.

- At the request of the Director, preparing advance issue papers for the Secretary for all reportable enforcement actions involving a civil penalty.

- Facilitating resolution of issues and actions through settlement between and among the parties and preparing appropriate documentation for issuance by the Director, SSA or the Administrator, NNSA.

- Maintaining a docket for (1) enforcement actions commencing with the filing of a PNOV; and (2) interpretations issued pursuant to 10 CFR Part 824.

2.4 Docketing

- A docket for enforcement actions will be maintained by the SP-23 commencing with the issuance of a PNOV. A docket for an enforcement action shall contain all documents required to be filed in the proceeding, including transcripts of any hearing conducted pursuant to 10 CFR Part 824.

- Subject to the provisions of law restricting the public disclosure of certain information, disclosure of records of enforcement actions will be made. The cost of duplicating documents shall be borne by the person seeking copies of such documents. The Director may waive this cost in appropriate cases.

2.5 Security Incident Coordinators

A key to effective communications, integration, and the successful implementation of the enforcement process is to have accurate and timely information. As outlined in this process, Security Incident Coordinators are located at each contractor facility (e.g., plant, laboratory,

etc.). Examples of activities currently performed by security incident personnel that will continue to be performed include, but are not limited to, the following:

- Assuring the flow of relevant, accurate and precise information between the Field and Headquarters Elements.

- Collecting information or coordinating with personnel to provide information and collaborate with the Security Enforcement Staff in evaluating the facts surrounding incidents of security concern and potential noncompliances.

- Coordinating the identification of personnel for technical support when necessary to bring an issue to closure.

- Providing status of closure and corrective action to classified information security noncompliances (incidents of security concern).

Federal line management personnel are routinely involved with the contractor operations on a day-to-day basis. Part of their responsibilities may include monitoring the contractor and thus they may feel a conflict in supporting enforcement activities. However, their roles should not be viewed as being in conflict with the enforcement activities. Federal personnel have an obligation to identify significant noncompliances with regulatory requirements to the contractor, the site, and line management and to ensure that appropriate corrective actions are taken. To the extent that such matters involve security enforcement issues, the contractor is responsible to formally report the noncompliances to the Department. Potential contractor noncompliances identified by DOE personnel should be communicated to the contractor for appropriate reporting. If it is learned the contractor declined to report a potential noncompliance and DOE believes further review is necessary to resolve the issue, the Security Incident Coordinator should, in concert with line management, communicate the issue directly to HQ and the Security Enforcement Staff, as appropriate for evaluation.

2.6 General Counsel

The General Counsel is the DOE Official responsible for formulating and issuing any interpretation (legal) concerning 10 CFR Part 824 or classified information security requirement. The General Counsel may utilize any procedure deemed appropriate to comply with these responsibilities.

2.7 Hearing Officer

The Hearing Officer is an Administrative Law Judge assigned to preside at hearings that are held under 10 CFR Part 824. The roles, responsibilities and procedures associated with a hearing are specified in 10 CFR Part 824.8, which describes the selection and duties of the Hearing Counsel and the Hearing Officer.

CHAPTER 3: IDENTIFICATION, EVALUATION AND INVESTIGATION OF NONCOMPLIANCES

3.1 Procedures for the Identification of Classified Information Security Noncompliances

Conditions that may not be in compliance with classified security information requirements may be identified through various activities. Examples include but are not limited to:

- An incident of security concern that is reported pursuant to DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management, Section N.*
- Formal inspections, surveys, and appraisals
- Special reports from DOE Headquarters or Field Elements
- Information or reports provided by the DOE Office of the Inspector General
- Allegations communicated to DOE from outside the Department
- Media reports of security incidents involving classified information
- Congressional inquiries
- Information from other agencies or state and local officials.

It is anticipated that the primary source of noncompliance information will be self-reporting by the contractors, because 10 CFR Part 824 provides positive incentives for the prompt identification and reporting of all potential classified information security violations. The primary vehicle that will be used by contractors for self-reporting are the existing procedures outlined in DOE Manual 470.4-1.

The contractor reporting will include, but not be limited to, a summary of the noncompliance, duration since incident occurrence, corrective actions, and other information related to the noncompliance to support DOE's review.

It should be noted that although the following sections refer to the identification, documentation, and significance of violations, the use of the term "violation" in the context of these sections refers to "potential violations" of DOE classified information security requirements. For the purposes of assessing an occurrence to determine whether action under 10 CFR Part 824 is warranted, a violation is considered to be any noncompliance with a DOE classified information security requirement, to include infractions. In general, an infraction will not lead to 10 CFR Part 824 processing; however, repeated, uncorrected infractions could result in such action. A

matter is only an actionable violation after an inquiry/investigation documents the development of information identifying relevant facts and circumstances surrounding the incident, and the rendering of a conclusion through the issuance of an Enforcement Letter or PNOV. The terms "noncompliance" and "violation" are essentially interchangeable in that both terms connote a failure to comply with an applicable classified information security requirement. In general, DOE uses the term "noncompliance" for matters in which the contractor has identified a condition that does not comply with classified information security requirements. Isolated minor noncompliances involving minimal or low classified information security significance will not be subject to enforcement actions but will be subject to periodic review, for such purposes as identifying recurring noncompliances.

3.2 Preliminary Evaluation of Noncompliances

The Security Enforcement Staff is reviews reports of significant security incidents [e.g. those categorized as Impact Management Index (IMI)-1, 2, or 3 pursuant to DOE M 470.4-1, *Safeguards and Security Porgram Planning and Management*] for consideration of more comprehensive investigation and potential enforcement action. The objectives of the review are:

- To confirm that a DOE classified information security requirement has actually been violated by reviewing the facts contained in the available information.

- To develop an initial evaluation of the security significance of the noncompliance to determine whether a more comprehensive investigation is warranted. This evaluation may be performed based upon the content of incident reports or ITAC reports, and any other incidents deemed of interest. For those incident and/or ITAC reports for IMI -1, 2, and 3 incidents associated with classified security information and other noncompliance conditions, DOE should perform an evaluation to determine whether to recommend the initiation of an investigation considering the evaluation of classified information security significance and other related factors. This decision usually involves interactive discussion with the Security Enforcement Staff and Security Incident Coordinators assigned to the Headquarters and/or Field Element and potentially an incident review meeting.

The Security Enforcement Staff will submit recommendations to the Director If the evaluation concludes that a more comprehensive investigation is required for consideration of enforcement action, an investigation is recommended. Guidance for these investigations is contained in the following section.

3.3 Investigation of Potential Violations

DOE investigates noncompliances to ascertain the facts, circumstances, and security significance of an incident of security concern involving classified information. During the conduct of an investigation, DOE may request documentation from the contractor, interview contractor workers and line management, conduct an onsite visit to obtain necessary facts and inspect the physical plant as well as related operations. Other DOE Headquarters and Field Element personnel may be requested to assist the Enforcement Staff in obtaining and reviewing the information. The conclusion of the investigation report will state the potential security

significance of the noncompliance. Additionally, the "next steps" recommendation will be made to the Director and Administrator, NNSA, as appropriate.

3.3.1 Investigating the Circumstances of the Noncompliance

Upon identification of a noncompliance that discloses a violation of a classified information protection requirement, the Security Enforcement Staff reviews all available documentation. If it is determined that the noncompliance warrants an investigation, the facts surrounding the matter are investigated and assembled. The investigation documentation should contain a detailed discussion of the facts that substantiate any classified information security issues and violations of classified information security requirements subject to DOE enforcement actions. There may be a need to supplement information initially received from other sources (e.g., local inquiry reports, inspection or survey reports).

3.3.2 Considering the Significance of the Classified Information Security Violation

DOE imposes sanctions commensurate with the severity of the violation. Once the circumstances surrounding a violation are understood and documented, the significance and the commensurate severity level are determined as part of the investigation.

In determining the significance of a classified information security violation, the documented evaluation should consider the potential impact on national security. If the Program Secretarial Office completed a damage assessment, it is considered during the course of the enforcement process. Additionally, any managerial policies and practices that may represent contributing factors must be considered. Consideration should be given to the matter as a whole, in light of the circumstances surrounding the violation. There may be cases in which the impact is low, but the failures of management are significant. Therefore, the severity level may be based upon the management failure(s) and not simply the low impact on national security. The following are examples of some factors that should be considered:

- Did the violation actually or potentially have an impact on our national security? A violation that involves no actual risk but that could have had an impact on national security may be very significant, depending upon the risk of the potential threat (i.e., its likelihood) and the possible consequences involved.

- What was the root cause of the violation? Was it caused by training deficiencies? Failure to follow procedures? Inadequate procedures? Failure to properly follow up on activities or commitments? These broader programmatic weaknesses may have more significance than the present violation.

- Is the violation an isolated incident or were there multiple examples of similar violations in the same time frame? Is it indicative of a management or programmatic breakdown? Management or programmatic breakdowns may be more severe than an isolated incident.

- Was management aware of or involved in the violation, and, if it was involved, at what level of management and to what extent? Violations in which management was directly involved

may be more significant than those of which management was unaware. Violations involving upper-level management should be considered more significant than those involving first-line supervisors. Inattentiveness on the part of management should also be considered, i.e., should management have been aware of the violation?

- What was the duration of the violation? If the condition existed for an extended period without discovery and correction, the risk generally is proportional to the duration of the violation, and the severity level of the violation should be increased.

- Was DOE notified promptly and provided complete information by the contractor when a violation was found? Delay in providing a comprehensive report to DOE may indicate lack of contractor initiative to understand the significance of the violation at a facility. Furthermore, failure of a contractor to report a violation to DOE in accordance with established reporting requirements may be considered a violation itself, in addition to the violation that occurred.

- Was the violation inadvertent or did it involve willfulness, and, if it did, to what extent? (See Section 6.3 for guidance regarding willful violations.)

- Was the violation related to a condition in a Compliance Order? These violations may be more significant because contractors have had prior notice of the violation and have not taken appropriate actions to correct it after having been directed to do so by the Secretary.

- Did the actual or potential impact involve severe consequences to our national security or involve lesser, but still substantial consequences?

3.3.3 Repetitive Violations

Repetitive violations are a concern because DOE expects a contractor's corrective actions to be effective in eliminating the source of the problem causing the violation. DOE expects contractors to learn from their past failures and not depend on DOE's assessment programs to identify and correct violations of classified information security requirements. Therefore, special attention is appropriate for repetitive violations, and escalated action should be considered. At the same time, it is recognized that there are many different circumstances that need to be considered. The following general guidance is provided (it should be noted that for purposes of this enforcement procedure, the term "repetitive" violations is interchangeable with the term "similar" violations):

- A "similar" or "repetitive" violation is defined as a violation that reasonably could have been prevented by a contractor's corrective actions for a previous noncompliance condition or violation of classified information security requirements involving similar circumstances and root causes and which occurred within a reasonable period of time.

- Previous noncompliance reports, enforcement actions, assessment reports, or "open items" listings from assessment reports, etc., should be used as appropriate to evaluate the contractor's prior enforcement history, including noncompliance items, to identify repetitive violations.

The severity level may be increased based on consideration of the frequency of examples of the violation in the same time frame, the number of times the violation has occurred, the similarity of violations and their root causes, the elapsed time between similar violations, and the extent to which previous corrective actions for similar violations were effective in preventing recurrence. The purpose of a decision to increase the severity level of a repetitive or extended violation is to emphasize the importance of DOE contractors' identifying violations and implementing effective corrective actions that address the root cause of the incident of security concern and prevent recurrence. The relative weight given to each of these factors in arriving at the appropriate severity level will be dependent on the circumstances of each case.

3.3.4 Incorporating Related Violations

During the course of the development of an enforcement action, additional information may be developed by DOE or the contractor involving other violations of DOE classified information security requirements related to the action being considered for enforcement.

These related violations are to be incorporated, if practical, into the pending enforcement action. The purpose of such incorporation is to focus the contractor's attention on the problem area, ensure that all relevant violations are considered whenever enforcement action is being evaluated, and ensure that the safety significance of the classified information security violations is evaluated appropriately.

Related violations may be identified at any stage of the enforcement process. If new evidence is identified after the enforcement action has been transmitted to the contractor, the additional related findings are brought to the attention of the contractor through a supplemental PNOV. If inclusion in the current enforcement action is not considered feasible, the Director may initiate a separate enforcement action, making appropriate reference to the current one.

3.3.5 Incident Review Meeting/Preliminary Recommendations on Enforcement Action

The Director, SSA will convene a meeting composed of representatives from SSA, the Headquarters Program Office and DOE Field Element with responsibility for the contract involved with the violation, and GC (or NNSA GC, as appropriate) to review the facts of the case and associated investigative results. At this informal meeting the investigation of facts and circumstances will be considered and a conclusion and a recommendation on enforcement action will be made. The factors affecting classified information security significance, and any the history of performance by the contractor will also be considered. The proposed severity level and any proposed monetary civil penalty will also be discussed.

3.3.6 Enforcement Letters/Closure Letters

If the Department decides not to issue a notice of violation, an Enforcement Letter signed by the Director may be sent to communicate the basis of the decision not to pursue further enforcement action for a noncompliance. The letter is intended to point contractors to the desired level of

security performance. It may be used when the Director concludes that the specific noncompliance at issue is not of the level of significance warranted for issuance of a notice of violation. It typically describes how the contractor handled the circumstances surrounding the noncompliance and addresses additional areas requiring the contractor's attention and the Department's expectations for corrective action. The letter notifies the contractor that, when verification is received that corrective actions have been implemented, the Department will close the enforcement action. In the case of NNSA contractors or subcontractors, the letter takes the form of advising the contractor or subcontractor that the Director has consulted with the NNSA Administrator, who agrees that further enforcement action should not be pursued if verification is received that corrective actions have been implemented by the contractor or subcontractor.

As a result of some investigations, an Enforcement Letter may not be required. When the Department decides that a contractor has appropriately corrected a noncompliance and that the significance of the noncompliance is sufficiently low, it may close out an investigation. Closing out a noncompliance with or without an Enforcement Letter may only take place after the Director has issued a letter confirming that corrective actions have been completed. In the case of NNSA contractors or subcontractors, the Director's letter takes the form of confirming that corrective actions have been completed and advising that the Director has consulted with the NNSA Administrator, who agrees that no enforcement action should be pursued.

CHAPTER 4: ENFORCEMENT CONFERENCES

If the Director determines, after completion of all assessment and investigation activities, that there is a reasonable basis to believe that a violation has occurred, and that the violation may warrant a civil penalty, an informal Enforcement Conference is normally held with the contractor involved before taking enforcement action. The Director may also elect to hold an Enforcement Conference for potential violations that would not ordinarily warrant a civil penalty but that could, if repeated, lead to such action. The purpose of the conference is to assure the accuracy of the facts upon which the preliminary determination to consider enforcement action is based; discuss the potential or alleged violations, their significance and causes, and the nature of and schedule for the contractor's corrective actions; determine whether there are any aggravating or mitigating circumstances; and obtain other information to help determine the appropriate enforcement action.

If immediate enforcement action is necessary in the interest of the national security, such action will be taken prior to the Enforcement Conference, which may still be held after the necessary Departmental action has been taken.

4.1 Enforcement Actions That Generally Require Enforcement Conferences

An Enforcement Conference is normally held in any of the following cases:

- Potential civil penalty actions at any severity level
- Selected Severity Level III violations that, if repeated, could lead to an enforcement action at a higher severity level
- Recurring noncompliances
- A group of Severity Level III violations for which a civil penalty may be considered.

In addition, the Director has the discretion to require a conference in any other circumstance in which it is appropriate for the clarification of matters in controversy and/or may lead to an improvement in classified information security. A contractor may request a conference at any time and the request will be considered by the Director.

4.2 Scheduling and Notification of Enforcement Conferences

In general, if an Enforcement Conference is planned, it should be held before an Enforcement Letter or PNOV is issued. The conference should usually be scheduled within four weeks after completion of the SSA investigation that supports the basis for a possible enforcement action. Section 6.2 discusses special procedures for cases that have been referred to the Department of Justice. Such cases require coordination with the Department of Justice and approval of the Director, SSA before an Enforcement Conference is scheduled.

4.3 Attendance at Enforcement Conferences

DOE Personnel

- The Director chairs the Enforcement Conference, and selected Security Enforcement Staff members attend.

- A representative of the Cognizant Headquarters Element and appropriate Field Element management representatives should attend the Enforcement Conference to provide input regarding the security significance of the violation, root causes, special circumstances, and comprehensiveness of corrective actions.

- At the request of the Director:

    - Representatives of General Counsel/NNSA General Counsel will attend.
    - Investigatory organizations may attend.
    - Other personnel.

Contractor Personnel

Contractors may participate with representation of their choice.

Other Matters

- Enforcement Conferences are considered Official Use Only, Exemption 5 meetings and are intended to provide a forum for open and candid discussion regarding a potential enforcement action. Therefore, they are normally closed meetings between DOE and the contractor (including the parent organization's management). Media and the public are thus excluded from Enforcement Conferences, although in some instances, a press conference may be held afterwards or a press release issued if the Director, in consultation with the Secretary, concludes it is appropriate.
- If classified information may be disclosed or discussed, all individuals attending must have appropriate clearances.

4.4 Notification to Contractor of an Enforcement Conference

DOE will prepare a Notification of Scheduled Enforcement Conference to inform the contractor and Departmental personnel of the schedule. The notification should describe the agenda to be discussed to help focus on the issues and make the conference as meaningful as possible. It is important to ensure that the contractor understands what is expected at the conference. The notification should include:

- Schedule and location for the Enforcement Conference

- DOE attendees planned for the conference, and personnel who should attend from the contractor organization

- Summary of DOE's preliminary conclusions and the potential violation based on information received to date

- Any particular points or information the contractor should address in the Enforcement Conference

- If time permits, an outline or agenda of the specific issues to be discussed.

4.5 Conduct of Enforcement Conferences

DOE's understanding of the facts and circumstances surrounding the violation are discussed at the Enforcement Conference. These discussions should include the significance of the classified information security violation and the contractor's understanding of the violation (i.e., whether the contractor agrees that the violation occurred, and if not, what additional facts it believes are relevant). In addition, the contractor should explain the causes of the violation, its views of the significance of the classified information security violation, and the corrective actions taken to correct the immediate problems and to prevent future occurrences. If appropriate, any aggravating or mitigating factors should be discussed. The contractor should provide documented support of its positions if this information has not been submitted earlier. Although the contractor may provide information that may be relevant to determining severity levels and civil penalty amounts, in general the discussion does not focus on such issues as specific severity levels, civil penalty amounts, mitigation percentages, or the nature and content of any Departmental directives. If the contractor offers its views on such issues, the Director will explain that final decisions on such matters will be made subsequent to the enforcement conference and will be provided to the contractor at a later date.

4.6 Identification of Additional Violations

When additional information, disclosed during or after the Enforcement Conference, could lead to the identification of more violations, such information should be substantiated with probative evidence before it is included in a proposed enforcement action. In addition, the contractor should: (1) have an opportunity to discuss the apparent violation(s) in a subsequent informal enforcement conference before it is formalized; and (2) provide any additional relevant information. The Director may choose to schedule a follow-up Enforcement Conference.

4.7 Enforcement Conference Summary Report

After the Enforcement Conference, a brief report is prepared by the Enforcement Staff to document the discussions. It is not necessary to summarize all discussion, but all relevant points of discussion should be included. The summary report should include the following information, as applicable:

- The date and place of the enforcement conference

- A list of the enforcement conference attendees from DOE and the contractor
- A summary of the factual information which provided the basis for the violation
- A brief description of the contractor's position, (i.e., if the contractor agrees with the findings or if the contractor takes issue with the potential violation)
- A list of any documents presented at the conference
- A brief description of significant additions or corrections to the factual information which is the basis for the violation
- A brief description of any significant additional information affecting the management involvement or significance of each violation
- A description of any points of significant disagreement
- A brief description of the contractor's short-term and long-term corrective and remedial actions that it has implemented or has committed to implement
- An analysis of all of the above information establishing the Department's conclusion on the violation.

The summary report is especially important for cases in which new information is provided, errors are identified in the documented basis for the violation, or significant clarifications of information are provided.

This summary report should be prepared so that it may be issued to all DOE enforcement conference attendees at the time an enforcement determination has been rendered. The report should be clearly marked as "Official Use Only (OUO), Exemption 5."

CHAPTER 5: ENFORCEMENT ACTIONS

5.1 Preliminary and Final Notices of Violation

A Notice of Violation (preliminary or final) is a document setting forth the conclusion that one or more violations of classified information security requirements have occurred. Such a notice normally requires the recipient to provide a written response. If the recipient concedes the occurrence of the violation, it is required to describe corrective steps that have been taken and the results achieved; remedial actions to be taken to prevent recurrence; and the date by which full compliance will be achieved.

The Department uses the Notice of Violation as the standard method for formalizing the existence of a possible violation, and the Notice of Violation is to be issued in conjunction with the proposed imposition of a civil penalty. In certain limited instances, as described in this section, DOE may refrain from issuing an otherwise appropriate Notice of Violation. However, a Notice of Violation normally is issued for willful violations, and for violations where past corrective actions for similar violations have not been sufficient to prevent recurrence and there are no other mitigating circumstances.

5.1.1 Preparation of Preliminary Notice of Violation (PNOV)

A PNOV should include the following elements, as a minimum:

- A concise, clear statement of the requirement(s) that was violated (legal citation for the violation).

- A brief statement of the circumstances of the violation, including the date(s) of the violation and the facts to demonstrate that the requirement was not met (the "contrary to" paragraph). Each violation, including a violation with multiple examples, will usually contain a single "contrary to" statement.

- The severity level proposed for the violation, or problem area, if violations are classified in the aggregate.

- The proposed remedy for each violation, including the amount of any civil penalty, if proposed. If more than one violation is involved, the amount of the penalty is apportioned for each violation.

- A statement of the contractor's right to submit a written reply to the Director, SSA within 30 calendar days of receipt of the PNOV. In cases where the PNOV is issued by the Administrator, NNSA, the contractor should be instructed to provide a copy of any response to the Director.

The "contrary to" paragraph should clearly demonstrate how the DOE classified information security requirement was not met. When appropriate, specific reference should be made to inadequacies in underlying programs or plans that implement the requirement. The PNOV (or

the Final Notice of Violation, or FNOV; see Section 5.1.4) also informs the contractor of the response required to DOE and, if applicable, of the contractor's option to request mitigation for any or all of any penalties being proposed.

The Appendix C Checklist should be consulted for guidance in preparing an enforcement action.

5.1.2 Transmitting PNOV to Contractor

The cover letter transmitting the PNOV to the contractor should include sufficient factual information described in "executive summary" format to help contractor management understand DOE's classified information security concerns, how DOE determined the sanctions that it is proposing, and where DOE concludes the contractor should focus attention to improve performance. The letter should be specific enough that the contractor receives a clear message as to how the Department has applied the *General Statement of Enforcement Policy* from Annex A to 10 CFR Part 824, and should clearly indicate which of the contractor's actions reflect good performance and which actions require additional attention. The letter should include the following elements, as appropriate:

- When and where an inspection or assessment was conducted.

- Who identified the violation, i.e., the contractor, DOE, or other external or internal sources (and reference to related reports)

- If and how the violation was reported.

- When and where an Enforcement Conference was conducted and reference to the conference report.

- A description of the violation(s), including the DOE requirements violated, the duration of the violation(s), the operational mode of the facility at the time of the violation(s), if applicable, the apparent root cause of the violation(s), and any other major attributes of the violation(s) necessary for supporting a determination of the significance of the classified information security violation(s).

- A discussion of the significance of the violation, including both the technical and the management failures, as appropriate, and how the significance of the violation led to the determination of the severity level.

- An analysis of any factors, such as management cooperation, management deficiencies or willfulness that caused the severity level to be escalated or decreased from the normal severity level for the type of violation. For those cases in which violations are aggregated based on management breakdowns (i.e., where there are multiple violations), the discussion should indicate that the violations are categorized as a Severity Level (X) <u>problem</u> rather than a Severity Level (X) <u>violation.</u> (The PNOV should also be categorized in this manner.)

- A description of the status of compliance or corrective actions to date, or the date when compliance will be achieved; e.g., "DOE recognizes that immediate corrective action was

taken when the violation was identified," "corrective actions have been initiated and appear acceptable," or "facility curtailed operation until completion of corrective actions." Special emphasis in this area is necessary when DOE is considering a decision on restart of operations. Any compensatory measures or corrective actions prior to restart should be addressed.

- A statement of the results that DOE expects to achieve through issuance of the proposed enforcement action, focusing on correction of the underlying problem(s) addressed by the violation(s).

- A discussion of the application of the adjustment factors, including the reasons for mitigation or escalation of the base civil penalty. The discussion should be specific and should address each of the factors for which mitigation or escalation of the base civil penalty was deemed appropriate, including those cases in which weighing all the factors resulted in no change to the base civil penalty.

- A description of the response that is necessary from the contractor and the time within which it is expected to be received. The paragraph discussing the response required should be expanded if a particular response is desired.

- A statement that DOE will determine what, if any, further enforcement action is required after review of the contractor's response to the PNOV, proposed corrective actions, and results of future assessments.

5.1.3 Settlement with Contractor

In accordance with 10 CFR Part 824, DOE will consider the settlement of any enforcement action or proceeding at any time during the enforcement process.
The Director may enter into a settlement, with or without conditions, of an enforcement proceeding at any time if the settlement is consistent with the objectives of DOE's classified information protection requirements.

The terms of settlement will be set forth in a Final Order signed by the Director or the NNSA Administrator and the contractor. A press release may be issued advising the public that the matter has been resolved.

Admission of Violation

- *For Enforcement Action with No Civil Monetary Penalty*: If the contractor admits that the violation(s) occurred as stated in the PNOV, the Director, in coordination with DOE program office, reviews the contractor's response for the adequacy of corrective actions and requests additional information from the contractor if necessary. In determining whether appropriate corrective actions have been taken, consideration should be given to proper contractor identification of the root cause(s) of the violation(s). The Director may consult with the NNSA, Headquarters and/or Field Element responsible for the contractor's activities. If there is an admission, however, it is generally unnecessary to issue an FNOV since the PNOV will become final.

- *For Enforcement Action with Civil Monetary Penalty:* If the contractor admits that the violation(s) occurred as stated in the PNOV and does not contest the civil penalty, the Director reviews the contractor's corrective actions in a manner similar to that for cases proposed without civil penalties. The PNOV becomes an FNOV without further action. Upon receipt of proof of payment for the civil penalty, the Director sends the contractor a letter acknowledging receipt of the monetary penalty and stating that the corrective actions described in the contractor's response will be examined during future assessments. Payment of the civil penalty will close the action; however, if the security noncompliance persists, a new action under 10 CFR Part 824 may be initiated.

Contention of Proposed Enforcement Action

The contractor may challenge DOE's facts or conclusions regarding the PNOV action by taking one or more of the following steps:

a. Dispute one or more of the facts or conclusions underlying a violation.

b. Dispute one or more of the violations.

c. Challenge DOE's conclusion regarding the significance or assigned severity level of the violation(s).

d. Request mitigation of the proposed civil penalty.

e. Dispute the proposed enforcement action but pay the civil penalty in order to resolve the matter in controversy.

- *For Enforcement Action with No Civil Monetary Penalty:* Each response should be carefully reviewed to ensure that DOE's action was appropriate. The Director prepares a response to the contractor addressing the each item that the contractor has challenged. Even if the contractor's response does not present new information, if an error in the enforcement action is identified, it should be corrected and documented. If the contractor presents additional information not previously disclosed, a more detailed response may be appropriate. The Director's response should consider the timeliness of the provision of information not previously disclosed. The Director may consult with NNSA Administrator or the Headquarters or Field Element responsible for the contractor's activities.

  Contractor responses that contest enforcement actions should be acknowledged by the Director within 30 days. If appropriate, an FNOV may also be issued by the Director or the Administrator, NNSA, at that time.

- *For Enforcement Action with Civil Monetary Penalty:* If the contractor challenges some aspect of the proposed enforcement action and does not pay the proposed civil penalty, the Director reviews the contractor's response and prepares a written evaluation of that response. The evaluation should address the contractor's points of contention and should include a restatement of each disputed violation, a summary of the contractor's position concerning

each disputed violation, the Department's evaluation of each position, and the conclusion. The Director may consult with NNSA Administrator or the Headquarters or Field Element responsible for the contractor's activities. If information is provided that changes the conclusion set forth in the PNOV, the basis for such reconsideration and conclusions should be set forth in the FNOV. In addition to the evaluation, the Security Enforcement Staff will prepare for the Director's signature: a transmittal letter, FNOV and the imposition of Monetary Civil Penalty within approximately 30 days of receipt of the contractor's response. FNOVs for NNSA contractors will be signed by the Administrator, NNSA.

If a contractor challenges some aspect of the proposed enforcement action but pays the civil penalty, the Director should review the contractor's points of contention. If the contractor presents additional information not previously disclosed, then careful consideration should be given to the appropriateness of the original proposed substantive action. In addition, the Security Enforcement Staff should prepare a response for possible inclusion in the acknowledgement letter sent by the Director. The Director may consult with NNSA Administrator or the Headquarters or Field Element responsible for the contractor's activities. However, if the contractor's response does not contain new information, then the Director should provide a brief response addressing only those issues that are significant and appropriate along with an assessment of the contractor's corrective actions. Even if the contractor's response does not present new information, if an error in the enforcement action is identified, it should be corrected. Contractor responses that contest enforcement actions but pay civil penalties should be acknowledged, usually within 30 days.

If the contractor has paid a monetary penalty and then, based on the above review of the contractor's response, it appears that part or the entire penalty was clearly paid in error, the portion of payment improperly assessed should be returned to the contractor. In such a case, the Director advises the contractor and arranges to have a check issued from the appropriate government office. After it is determined that the check has been issued, the Director sends a letter to the contractor explaining the rescission to the civil monetary penalty and concludes the proceeding in accordance with the facts of the case.

Denial of Violation

If there is a denial in full by the contractor that a violation has occurred, the Director conducts a complete review of the case file prior to a decision to withdraw the PNOV or release the FNOV based on the evidence addressed (see Section 5.1.4). Pursuant to 10 CFR Part 824, the contractor's sole remedy under circumstances where an FNOV has been issued and a civil penalty imposed is to request an on-the-record adjudication. The contractor is required to file a written answer to the FNOV, which sets forth specific guidance regarding the contents of the answer. The matter then proceeds at the direction of the Director.

5.1.4 Final Notice of Violation

Upon evaluation of contractor responses and all other relevant evidence, the Director or, as appropriate, in consultation with the Administrator, NNSA, may take one of the following actions:

- Rescind all, or part, of the proposed civil penalty
- Determine that no violation has occurred and rescind the PNOV
- Issue the FNOV and impose a civil penalty, as authorized by law.

The FNOV generally follows the same format and content as the PNOV, but is updated based on any new information to reflect final conclusions. Signatures of other DOE and/or NNSA officials are obtained as necessary prior to issuance of the FNOV. It should be noted that issuance of an FNOV in matters in which the facts and penalties are uncontested is discretionary since the PNOV will constitute an FNOV under such circumstances.

5.2 Severity Level

Violations of classified information security requirements are categorized in three levels of severity to identify their relatlive security significance. The *General Statement of Enforcement Policy*, 10 CFR Part 824, Appendix A, provides guidance on the categorization of severity level for violations, based largely on security significance and other factors related to the violation. Severity level definitions set forth in 10 CFR Part 824, Appendix A, will be used. A severity level may be adjusted up or down by the Department based on the circumstances of the particular violation. This can include consideration of multiple violations in the aggregate.

5.2.1 Aggregation of Violations

A group of violations may be evaluated in the aggregate if: (1) they have the same underlying cause or are attributable to management deficiencies; or (2) they contributed to the same underlying effect; and (3) the resulting Severity Level is I, II or III.

Any circumstance involving numerous violations should be considered for aggregation at a Severity Level II or III and, when appropriate, Severity Level I. However, both the number and nature of the violations should be considered. Numerous violations that are related (for example, those involving training, procedures, information security evaluations, or management controls) should be considered for aggregation. A group of noncompliances can also be aggregated and designated as a violation at the appropriate severity level if the facts and circumstances merit such an action.

Aggregation of violations to a higher severity level should not be confused with the use of multiple examples in Notices of Violation or the use of the multiple occurrences in determining a severity level.

5.2.2 Severity Level I and II Violations

Severity Levels I and II are generally reserved for cases involving actual or potential compromise of classified information, or indicating the potential for such cases occurring due to management or programmatic issues. Specific considerations that may raise the severity level of a violation even in the absence of a significant risk include the following:

- Prior knowledge that the violation existed but was not corrected.

- Extended duration of a violation that was readily detectable by normal self-assessment activities.

- Multiple and/or repetitive examples of a violation evidencing a significant management failure to ensure programmatic implementation of regulatory requirements.

Programmatic deficiencies that could lead to such an adverse classified information security impact would normally be Severity Level II unless the potential or actual classified information security consequences to national security warrant Severity Level I. At times a violation leads to an incident of low impact or consequence to national security. If this violation was less significant because of fortuitous circumstances rather than being limited by discrete program controls, the violation would normally be considered a Severity Level II.

5.2.3 Penalty Mitigation Factors Not Affecting Severity Level

After the severity level is determined, factors such as the contractor's accurate timely reporting and prompt corrective action based upon root cause analysis are considered, where appropriate, as an adjustment of any civil penalty. Other factors that do not affect the severity level, but could affect the adjustment (up or down) of a base civil penalty are as follows:

- What role did DOE play in the violation? Did DOE approve the noncompliance condition? If so, was the approval in writing or was it oral? Was DOE previously aware of the noncompliance condition and condone it through inaction? Lack of DOE funding is not a basis for civil penalty mitigation. Deviations to classified information security requirements contained in an order or manual must be in writing and follow the process outlined in DOE M 470.4-1, *Safeguards and Security Program Planning and Management* in order to be valid.

- Were appropriate corrective actions taken by the contractor to prevent recurrence? Factors to be considered include the degree of initiative shown by the contractor, timeliness and appropriateness of actions taken, and proper root cause identification. Also, consideration is given to the comprehensiveness (broadly addressing areas of concern vs. narrowly focused) of the contractor's corrective actions.

5.2.4 Severity Level III Violations

The Enforcement Policy provides that Notices of Violation need not be issued for noncompliance items which are minor violations (e.g., infractions) of classified information security requirements. Such discretion is exercised so that the Department can focus its enforcement activities on matters that have greater actual or potential significant impact on classified information security violations and the national security. The Enforcement Policy encourages contractors to identify and correct violations and, at the same time, avoid unnecessary effort spent on the associated administrative work by the Department and its contractors that can be better spent on improving the classified information security requirements and the performance of them. Noncompliance items that do not result in Notices of Violation, however, must be tracked to identify repetitive conditions or to assess generic or facility-specific problems.

From an enforcement perspective, Severity Level III violations should be issued to contractors who are not exercising initiative in the identification and effective correction of noncompliances without the involvement of the Field or Headquarters Element. Further, Severity Level III violations should be considered for contractors which permit recurring noncompliances without taking effective corrective actions. Severity Level III enforcement actions generally should be focused on those issues that the contractor does not address aggressively and appropriately.

The Department may refrain from issuing a PNOV:

- If the contractor identifies and reports a noncompliance violation in a timely manner;
- If DOE is satisfied with the root cause analysis and corrective actions; and
- If the matter does not appear to be of a recurring nature, pose an extreme impact on national security, or have a potential to lead to a more serious national security impact.

However, these noncompliances must be monitored to assure whether appropriate corrective actions are taken to prevent recurrence. If such noncompliances are not properly addressed, they can be grouped and escalated to a Severity Level III violation.

If the actual or potential consequences to national security are minimal, associated noncompliances are generally considered as Severity Level III. Even if direct national security consequences are not readily apparent for each noncompliance, they may be collectively considered a Severity Level III violation if they indicate a programmatic deficiency.

5.3 Base Civil Penalties

In assessing a civil penalty, the table in the *General Statement of Enforcement Policy*, 10 CFR Part 824, Appendix A, should be used to determine the base civil penalty based on the severity level of the violation.

The *General Statement of Enforcement Policy* states that civil penalties are designed to emphasize the need for lasting remedial action, to deter future violations, and to underscore the importance of contractor self-identification, reporting, and correction of violations of nuclear classified information security/requirements. Furthermore, the imposition of civil penalties generally takes into account the gravity, circumstances, and extent of the violation, along with any history of prior similar violations and the degree of culpability. It may be appropriate to increase the size of the base penalty on the basis of the impact to national security and the size and nature of the contractor operations and program. Civil penalties are not normally proposed for Severity Level III violations, except in circumstances where a civil penalty may be appropriate to demonstrate the importance of adherence to the Department's classified information security requirements, or where violations are similar to previous violations for which the contractor did not take effective corrective actions.

Furthermore, the *General Statement of Enforcement Policy* states that in cases involving (1) ineffective contractor programs for identifying problem(s) or correcting them, (2) willfulness, (3)

flagrant DOE-identified violations, (4) repeated poor performance in an area of concern, or (5) serious breakdowns in management controls, the Department has discretion to assess a civil penalty up to the statutory limit of $100,000 per violation per day.

5.3.1 Applicability

A civil penalty is normally proposed for Severity Level I or II violations, absent mitigating circumstances, and for any willful violations of any classified information security requirement as outlined in 10 CFR Part 824. Civil penalties should be considered for Severity Level III violations that are similar to previous violations for which effective corrective actions were not taken.

5.3.2 Violation Grouping

Depending upon the circumstances of a case, assessment of violations may be considered in a number of ways:

- Each Severity Level I, II, or III violation may be assessed a separate civil penalty.
- Several violations stemming from the same cause or problem area may be evaluated in the aggregate, assigned a single severity level, and assessed a total civil penalty.
- If more than one cause or problem area is identified, separate civil penalties may be considered for each violation.
    - The determination of whether there is more than violation can be made by evaluating whether corrective actions for one violation would prevent recurrence of the other violation(s).
    - If corrective actions are required in more than one area, separate civil penalties may be assessed.
- Separate penalties may be assessed for separate violations stemming from a single problem area if the violations were separated over time.
- The determination to group violations or to consider each violation as separate is also a function of the significance of the case and the emphasis and message to be provided to the contractor.

5.4 Adjustment of Base Civil Penalty

After the appropriate base civil penalty is determined, the civil penalty adjustment factors outlined in the *General Statement of Enforcement Policy*, 10 CFR Part 824, Appendix A, are used to determine the magnitude of the civil monetary penalty that is to be assessed. The single most important goal of the DOE Enforcement Program is to encourage early identification, reporting, and prompt correction of classified information security deficiencies and violations by the contractors, rather than Department. Consequently, the Department provides substantial

incentive for the early self-identification, reporting, and correction of problems which constitute, or could lead to, violations of classified information security requirements. The base civil penalty may be increased up to the statutory limit, decreased, or completely mitigated based on the application of the adjustment factors.

Since the adjustment factors are additive, the penalty for any one violation could exceed the daily base civil penalty as specified in Table I of the *General Statement of Enforcement Policy*. However, in no instance can escalation cause the daily penalty to exceed the $100,000 per day statutory ceiling per violation. The following subsections should be used in conjunction with the guidance in the *General Statement of Enforcement Policy.*

5.4.1 Per-Day Provisions

10 CFR Part 824 establishes a maximum civil penalty that can be imposed of $100,000 per violation per day. Thus, a noncompliance condition that exists for several days could be pursued by DOE as an enforcement action with a base civil penalty substantially above $100,000. The Department will use the Table 1 Severity Level values as the base starting point, and consider multiples of that value based on the number of days that the noncompliance condition existed. A per-day calculation of a civil penalty is normally considered:

- When the significance of the violations is such that use of a single-day base civil penalty is not sufficient to convey the seriousness of the violation or circumstances leading to the violations, and

- When sufficient opportunities existed to identify the violations.

Examples of substantial opportunity to identify the violation include the following:

- Management was aware of the violation and chose not to take appropriate action to remedy the problem and failed to report the violation to DOE.

- The violation existed for an extended period as a result of a failure to perform established surveillance, assessment or security-related quality assurance activities that, if performed as required, would have resulted in timely detection of the problem.

Reduction of up to 50% of the base civil penalty shown in Table 1 may be given when a contractor identifies the violation and promptly reports the violation to DOE. In weighing this factor, consideration will be given to, among other things:

- Whether prior opportunities existed to discover the violation, and if so, the age and number of such opportunities

- The extent to which proper contractor controls should have identified or prevented the violation

- Whether discovery of the violation resulted from a contractor self-monitoring activity

- The extent of DOE involvement in discovering the violation or prompting the contractor to identify the violation

- The promptness and completeness of any required report.

DOE does not normally give credit for a contractor's corrective actions if DOE intervention was required to broaden the scope or increase the extent of the corrective actions. Mitigation is not appropriate merely because immediate actions are taken to correct a condition, since basic corrective actions to resolve an identified problem are necessary as a matter of routine. Adequate attention to the broader implications or underlying programmatic deficiencies must also be addressed if such are indicated by the occurrence or recent history.

5.4.2 Multiple Separate Violations

DOE may cite separately and impose civil penalties for each of the multiple violations in a citation, even if they are related to a single event. Each violation is subject to the statutory limit of $100,000 per day. This means, for example, that a single event involving a violation of classified information security requirements, and also involving violation of security-related quality assurance requirements, could result in a PNOV citing these violations and include a civil penalty associated with each.

The significance of a particular occurrence and the circumstances of the violations may dictate that DOE identify the multiple violations involved and impose civil penalties for each violation. This action communicates the right emphasis on the significance of the violations and the attention that is required by the contractor to correct the conditions that led to the violations.

A particular violation case is not closed by DOE when a contractor concedes the violation and pays any civil penalty. DOE will keep a violation case open until it has confirmed that appropriate corrective actions have been completed. If corrective actions are not completed in a timely manner, DOE could decide to take further enforcement action, such as escalating the civil penalty contained in the FNOV.

5.4.3 Identification and Reporting

This factor may be used to decrease a civil penalty for a violation by up to 50% if a contractor promptly identifies its occurrence and promptly reports the violation to DOE. No credit is given if timely effort to restore compliance with the regulatory requirement is not undertaken.

It should be recognized that a self-disclosing event, in which the event itself discloses problems that represent violations of classified information security requirements, does not represent contractor initiative in self-identifying the problems. DOE's priority is for contractor initiative to identify such problems before they lead to events with actual or potential classified information security consequences. The disclosure by an event that such problems exist does not constitute self-identification for the purposes of applying enforcement mitigation considerations. DOE's policy on consideration of self-disclosing events is addressed in the Enforcement Policy.

In weighing the factor of mitigation for self-identification and reporting, consideration should be given to, among other things, prior knowledge of the noncompliance condition, the opportunity available to discover the violation, ease of discovery, and the promptness and completeness of any required report. No consideration should be given to a reduction in penalty if the contractor does not take immediate action to correct the problem upon discovery.

If the contractor identifies the violation but the Department does not decrease the civil penalty on the basis of that identification, the discussion in the cover letter to the contractor should very specifically and clearly articulate the reason for not mitigating the civil penalty. For example, the discussion might explain why it is reasonable to conclude that the contractor should have identified the violation sooner. In general, mitigation should not be considered if the report is received after an event that is considered a self-disclosing event.

In addition, if a separate civil penalty is being assessed for a reporting violation, it is not appropriate to increase the civil penalty on the basis of the identification and reporting factor if a contractor fails to make a required report or issues a late report of an event. Instead, a separate violation and associated civil penalty should be considered, consistent with the Enforcement Policy.

5.4.4 Corrective Action

This factor may be used to either decrease or increase a base civil penalty by up to 50% depending on the promptness and extent to which the contractor takes corrective action, including actions to prevent recurrence.

Some corrective actions are always expected to remediate a problem. Mitigation is appropriate only when corrective actions are comprehensive in nature rather than being narrowly focused on the noncompliance issue. Generally the contractor would require a clear understanding of the scope of the violation in order for its corrective actions to be considered under this factor. Application of this factor should consider (depending on the circumstances) the timeliness of the actions, the contractor's initiative to take action, the rigor with which the contractor identifies the root cause(s), and the comprehensiveness of the corrective actions. Corrective action that is inappropriately focused normally results in no adjustment to the amount of the civil penalty.

Mitigation of the base civil penalty may be appropriate if there was essentially no other reasonable action that the contractor could have taken. If the base civil penalty is not reduced, the cover letter may include an explanation of what further action the contractor should have taken.

Escalation of the base civil penalty may be appropriate for cases in which the contractor's corrective actions are considered untimely and inadequate due to the contractor's failure to fully recognize or understand the extent of the problem. A separate civil penalty assessment may be appropriate based on the contractor's failure to take adequate corrective actions after it is clear that the contractor should have recognized the condition adverse to classified information security requirements and its impact on national security.

5.4.5 Multiple Examples/Repetitive Violations

As a general rule, multiple examples of the same violation of a specific requirement during the period covered by an inspection or assessment should be included in one citation. The "contrary to" paragraph should generally state the violation and then identify the examples. These examples may reference failures to comply with implementing plans or programs which are included in the classified information security requirements. When the examples of a particular violation are numerous, sufficient examples should be cited to convey the scope of the violation and programmatic breakdowns, and to provide a basis for assessing the effectiveness of the contractor's corrective actions. Normally three to five examples should be adequate. However, in cases where there are clearly several Severity Level(s) I and/or II violations, each violation should be cited separately. Use of multiple examples in Notices should not be confused with either (1) the concept of aggregation of violations or (2) the use of multiple occurrences for assessing severity level.

The cover letter transmitting the enforcement action should state that repetitive violations were considered and should identify those past violations specifically. It should note further that in the absence of lasting corrective action, more significant enforcement action may be taken.

5.4.6 Exercise of Discretion

Because the Department wants to encourage and support contractor initiative for prompt self-identification, reporting and correction of problems, DOE may exercise discretion as follows:

The Department may refrain from issuing a civil penalty for a violation that meets all of the following criteria:

- The noncompliance is promptly identified by the contractor, prior to some self-disclosing event, and reported in accordance with DOE Manual 470.4-1 consistent with reporting thresholds established in that Manual.
- The violation is not willful or a violation that could not reasonably have been prevented by the contractor's corrective actions for a previous violation.
- The contractor, upon discovery of the noncompliance, took, or began to take, prompt and appropriate action to correct the noncompliance.
- The contractor took, or has agreed to take, remedial action satisfactory to the Department to preclude recurrence of the violation and the underlying conditions which caused it.
- The violation is not a repeat violation or similar to a previous one for which appropriate corrective actions to preclude recurrence should have been taken.

DOE may refrain from proposing a civil penalty for a violation involving a past problem that meets all of the following criteria:

- It was identified by a DOE contractor as a result of a formal process that had a defined scope and time requirement that is being aggressively implemented and reported.

- Comprehensive corrective actions have been taken or are well under way within a reasonable time following identification.

- It was not likely to be identified by routine contractor efforts, such as normal surveillance, self-monitoring or security-related quality assurance activities.

DOE may reduce the severity level of violations involving not-for-profit entities to the extent that they have satisfactorily met the mitigation factors discussed above.

DOE will not issue a Notice of Violation for cases in which the violation discovered by DOE or the contractor cannot reasonably be linked to the conduct of that contractor in the operation of the DOE facility involved. This exercise of discretion is conditioned on prompt and appropriate remedial action taken by the contractor upon identification of the past violation. This does not include a past violation where actions by the present contractor should have identified the violation previously.

5.4.7 Refraining from Issuing a Civil Penalty

Further discretion is provided the Department in the issuance of civil penalties in the *General Statement of Enforcement Policy*. If specified criteria are met (as summarized here), the Department may, when issuing a PNOV, refrain from issuing a civil penalty in order to encourage prompt self-reporting and correction of violations, and to otherwise further the interests of justice through recognition of proper attributes of voluntary compliance. In addition, the violation may not be willful or one that could reasonably be expected to have been corrected by the contractor's correction of a previous violation. Finally, corrective actions by the contractor must preclude recurrence of the violation and the underlying conditions that caused it.

In addition, DOE may refrain from issuing a civil penalty for past problems that the contractor identified as a result of special reviews and inspections. These reviews must have a well-defined scope and schedule, and comprehensive corrective actions must be promptly taken. These problems must be the type that would not likely be identified in normal surveillance or security-related quality assurance activities by the contractor.

In these situations, the imposition of a civil penalty might deter the voluntary compliance aspects of the DOE enforcement program and other objectives of DOE classified information security initiatives. These programmatic objectives should be noted in the PNOV as further reasons why a monetary penalty was not imposed.

5.4.8 Ability of Contractor to Pay Civil Penalty

Although the table in the *General Statement of Enforcement Policy* generally takes into account the classified information security significance of a violation as a primary consideration in assessing a civil penalty, the contractor's (including subcontractors, vendors, and suppliers) ability to pay may be a secondary consideration. It is not the purpose of DOE enforcement actions to be so severe as to put the contractor into bankruptcy. Contract termination, rather than civil penalties, is used to terminate contractor activities within the Department. However, the

burden of proving inability to pay is on the contractor and must be conclusively demonstrated by a present financial condition—not a future condition. If it appears that the economic impact of a civil penalty might put a contractor into bankruptcy, interfere with a contractor's ability to safely and securely conduct activities and/or correct the violation to bring its program into full regulatory compliance, it may be appropriate to decrease the base civil penalty. However, it is expected that this discretion would rarely be used. Economic hardship must be clearly demonstrated by the contractor. The Director may also request assistance from other Departmental Elements, e.g., NNSA, to substantiate a mitigating financial condition. Furthermore, administrative actions, such as determination of award fees when provided for in DOE contracts, will be considered separately from any civil penalties imposed. Likewise, imposition of a civil penalty will be based on the circumstances of each case, unaffected by any award fee determination.

5.5 Administrative Matters

5.5.1 Assignment of Enforcement Action Number

Security Enforcement Action (SEA) numbers are assigned to all proposed enforcement actions after a decision is made to issue a PNOV. It is a method of administratively docketing and tracking cases. The action numbers are assigned sequentially according to the year of issuance (i.e., SEA 05-01, SEA 05-02, etc.). Once an SEA number has been assigned to an enforcement matter, all filings, memoranda, and correspondence for that case should include the case name and its complete SEA number.

5.5.2 Press Releases

Press releases may be issued for PNOVs and FNOVs at the discretion of DOE senior management. The need for a press release and the timing and method of its release is determined in cooperation with the Office of Public Affairs, the Secretary, and the Deputy Secretary, as appropriate. Generally, a press release will not be issued until the contractor has been in receipt of the enforcement action for 48 hours.

5.5.3 Release of Official Use Only, Exemption 5 Enforcement Information to Contractors and to the Public

The Director, in consultation with appropriate Departmental officials, is responsible for all decisions regarding the release of OUO, Exemption 5 information to contractors and to the public. Such information includes matters such as potential severity level of the alleged violation, civil penalty amount, and the nature/context of a PNOV. As a general rule:

- No information is released to the public prior to the release of a PNOV.

- Enforcement information is only released to the contractor: (1) to permit preparation for an Enforcement Conference or (2) to ensure that prompt correction actions are taken to obtain compliance. In other circumstances, however, such information should not be made available to the contractor prior to the release of a PNOV. Upon completion of service of a PNOV, the DOE transmittal letter and PNOV are placed on the SSA web site on the Internet.

CHAPTER 6: ADDITIONAL ENFORCEMENT GUIDANCE

6.1 Notices of Violation for Subcontractors and Suppliers

Notices of Violation (both PNOV and FNOV) are used for subcontractors and suppliers who fail to meet the classified information security requirements. Enforcement for subcontractors and suppliers is addressed in the Enforcement Policy (10 CFR Part 824, Appendix A). Violations of such requirements are subject to the same enforcement process described in this enforcement procedure.

Additionally, classified information security requirements may be contained in contract requirements with DOE contractors and are not directly imposed by DOE on the subcontractors and suppliers. For example, a subcontractor may be required to have a classified matter protection and control (CMPC) program in order to perform work for the contractor. Violations of that CMPC program may subject the subcontractor to a 10 CFR Part 824 enforcement action. The PNOV for a subcontractor or supplier would be similar to that prepared for a DOE contractor, but will also include the following elements:

- Any contract terms that subject the subcontractor or supplier to DOE classified information security requirements and the severity level proposed for the violation or problem area will be specified.

- If the subcontractor or supplier to DOE is subject to classified information security requirements, the civil penalty proposed for each violation may apply equally to the prime contractor, if appropriate. If more than one violation is involved, it may be necessary to apportion the amount of the penalty for each violation.

The PNOV informs the subcontractor or supplier of the response required by DOE. The PNOV automatically becomes an FNOV if the subcontractor or supplier response does not contest the enforcement action.

If the violation of classified information security rules by the subcontractor or supplier has affected the work of the prime contractor, Notices of Violation to multiple parties may be issued for the same occurrence. Contractors have responsibility for the performance of their subcontractors through the oversight responsibilities of their CMPC programs. As with all cases, care should be exercised to determine the relevant facts in these circumstances and to assess responsibility in accordance with facts.

6.2 Department of Justice Referrals

6.2.1 Policy on Withholding Action

As a general policy, if a matter has been referred to the Department of Justice (DOJ), in the absence of an immediate need to take action for national security reasons, issuance of a DOE enforcement action should be held in abeyance. The purpose of this postponement is to avoid

potential compromise of, or conflict with, the DOJ investigation (case), pending DOJ concurrence that the enforcement action will not affect its prosecution. The Director, or designee, is responsible for coordinating enforcement matters with DOJ.

6.2.2 Department of Justice Declinations

It is expected that if DOJ determines that a referred case lacks prosecutorial merit, the DOE will be notified by a letter of declination and jurisdiction of the case will be returned to the Department. When this is received, the Director will then determine whether to proceed with enforcement action. Enforcement would then follow the same process described in this enforcement procedure.

6.3 Willful Violations

Violations involving **gross negligence, deception or willfulness** are treated more seriously, and the severity level would likely be escalated. Willful violations are of particular concern because the DOE Enforcement Program is based on encouraging DOE contractors to communicate with candor and openness. DOE contractors are expected to implement significant remedial measures in responding to willful violations in order to demonstrate recognition of the importance of the violation and to deter future willful violations. It should be clear that contractors are held accountable for the conduct of their employees.

Under the Enforcement Policy, a civil penalty is normally proposed for willful violations at any severity level. Every case involving a willful violation should be considered for an action, and may require referral to DOJ for consideration of criminal sanctions. Willful violations at any severity level are unacceptable and will not be tolerated. Even if a violation could be considered for enforcement discretion, a PNOV and civil penalty will be issued for willful violations.

A violation in which a contractor should have been aware of the requirements does not in itself necessarily represent a willful violation. However, as an example, if prior to taking the action, the contractor (through its employees) is informed or made aware that the action about to be taken would violate a classified information security requirement, plan, or procedure, and the contractor proceeded to take action without appropriate approvals, then the case would be considered a willful violation. Evidence that the contractor had prior warning can include documented notes or correspondence, as well as testimonial input such as interviews subsequent to the event. Another example of willfulness is intentional destruction of records. Each case involving a potential willful violation will be considered individually with respect to the unique facts associated with that case.

6.4 Employee Liability

The civil penalty provisions of 10 CFR Part 824 apply to DOE contractors, subcontractors and suppliers. Individual employees are not liable under 10 CFR Part 824.

6.5 Contractor Transition

From time to time, DOE must transition management and operations responsibility from one contractor to another and appropriate planning for the transition of compliance with classified information security requirements is necessary. The process of transition normally includes a period of review and due-diligence on the part of the incoming contractor. DOE's expectation is that the present contractor will have responsibility for compliance with DOE classified information security requirements during the period of their contract, up to the date of turnover to the new contractor. DOE could pursue enforcement action with the present contractor for any cases of noncompliance that occurred at any time during the period of their contract.

The incoming contractor is expected to assume full responsibility for secure operations and compliance with DOE classified information security requirements on the date they assume contract responsibility for the site or facility. This responsibility includes compliance with any implementation and program plans associated with classified information security requirements, as well as implementing policies, procedures, documents and controls. The incoming contractor is expected to identify, during their due-diligence review, any issues of compliance with DOE classified information security requirements, including implementation plans and programs. These issues must be addressed and resolved with the appropriate DOE program, site, or operations office management prior to assuming responsibility for management and operation of the site or facility.

The Department intends to exercise reasonable discretion in considering noncompliance issues that surface in the near term after the incoming contractor assumes responsibility, and that could not have reasonably been identified during the due-diligence period. DOE will generally forgo enforcement action during this early, near-term period if the contractor, upon identifying the condition, appropriately reports to DOE and responds with timely and effective corrective actions.